Safety Science 79 (2015) 213–228

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Structuring the safety case for unmanned aircraft system operations in non-segregated airspace

Reece A. Clothier [a,*], Brendan P. Williams [b,1], Neale L. Fulton [c]

[a] School of Aerospace, Mechanical and Manufacturing Engineering, RMIT University, Melbourne, VIC 3000, Australia
[b] Australian Research Centre for Aerospace Automation, Queensland University of Technology, Brisbane Airport, QLD 4008, Australia
[c] Commonwealth Scientific and Industrial Research Organisation, Canberra, ACT 2601, Australia

ARTICLE INFO

Article history:
Received 9 February 2015
Received in revised form 30 March 2015
Accepted 10 June 2015

Keywords:
Remotely piloted aircraft systems
Unmanned aircraft systems
Mid-air collision
Safety case
Barrier bow tie modelling

ABSTRACT

Routine access to non-segregated airspace is a key enabler for the civilian Unmanned Aircraft System (UAS) industry. Approvals for UAS operations in this airspace are contingent on the provision of a safety case, which details how the risk of a Mid-Air Collision (MAC) accident will be managed to an acceptable level. There is no accepted framework for structuring operational safety cases for UAS and this gives rise to a number of challenges to the application of the regulation by "safety target" approach. Further, a wide range of controls has been proposed for mitigating the risk, however the effectiveness of the controls is not known. A reconciliation and extension of existing causal models describing the MAC accident sequence is provided in this paper. A barrier bow tie model is developed as a means for structuring the safety case for generic UAS operations in non-segregated airspace. The model is applied to the classification of over 50 commonly used risk controls and the relationship between the control and the manner in which the reduction in MAC risk is achieved is determined. A case-study application is also presented validating the utility of the tool in the development and communication of safety cases for UAS operations in civilian airspace.

1. Introduction

In order for Unmanned Aircraft (UA) to gain routine access to non-segregated civil airspace it must be shown that their operations do not increase the risk to other airspace users or compromise existing safety levels (EUROCONTROL, 2012). Non-segregated airspace refers to the operation of UA outside of segregated airspace, where segregated airspace is defined as airspace of specified dimensions allocated for exclusive use to a specific user(s) (ICAO, 2011). The operation of an Unmanned Aircraft System (UAS) poses a number of safety hazards. The primary hazard of interest in this paper is that of a Mid-Air Collision (MAC) between an UA (the flying component of an UAS (ICAO, 2011)) and a Conventionally-Piloted Aircraft (CPA). Secondary hazards, which can occur as a result of the primary hazard, include evasive manoeuvring of aircraft, falling debris, fires, and vehicle accidents, *etc.*, (Clothier and Walker, 2014). These hazards pose potential for harm to a range of Entities of Value (EoV). Of particular interest to aviation safety authorities are those hazards that have the potential to cause an accident, more specifically, the death or serious injury of people, or significant damage or loss of the UA (refer to Annex 13 to the Chicago Convention (ICAO, 2010) for a comprehensive definition of an UAS accident). The relationships between the hazards and EoV are illustrated in Fig. 1. Not shown in Fig. 1 is the potential for collision avoidance manoeuvres to create new conflicts with other aircraft. The focus of this paper is on the primary accident scenario illustrated by the large solid arrows in Fig. 1.

For CPA the risks associated with the hazard of a MAC are managed through a framework of regulations pertaining to the training and licensing of personnel, equipage, aircraft operation, and the provision of Air Traffic Services (ATS). A similar framework of regulations specific to UAS has yet to be developed. It is widely agreed that UAS should operate "seamlessly" (CAA-UK, 2012; JAA, 2004) and "transparently" (CAA-UK, 2012; ICAO, 2011) within the Air Traffic Management System (ATMS). More specifically, UAS should interact with the ATMS in a similar manner to that of existing airspace users. From the perspectives of the Air Traffic Service Provider (ATSP) and other airspace users, an UAS should appear and behave no differently to that of a CPA. The requirement implies that UAS should be subject to the same personnel licensing, equipage, and rules of the air as that applicable to CPA. However,

* Corresponding author. Tel.: +61 3 9925 7007.
E-mail address: reece.clothier@rmit.edu.au (R.A. Clothier).
[1] Mr. Williams is on secondment to the Queensland University of Technology from Boeing Research & Technology, Australia.

http://dx.doi.org/10.1016/j.ssci.2015.06.007
0925-7535/

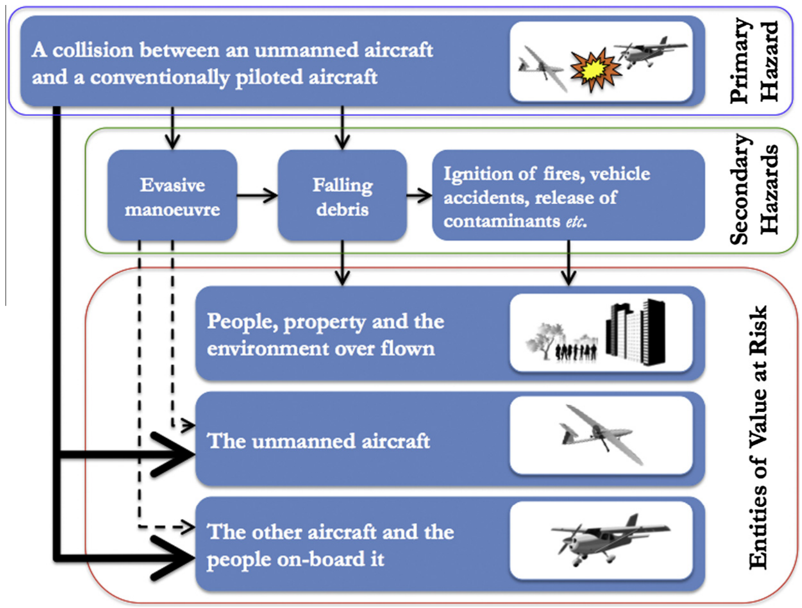

Fig. 1. Illustration of mid-air collision risk scenarios for a single conflicting pair of aircraft.

applying the same regulations to UAS may not be practicable or achieve the same safety outcomes. This is particularly the case for (1) UAS without a Detect-and-Avoid (DAA) capability, (2) small UA that are unable to meet equipage requirements due to size, weight and power constraints, and (3) UAS with unique airspace-use profiles.

An alternate approach, which is widely in use for the regulation of UAS operations today, is the "safety-target" (Haddon and Whittaker, 2002) approach. Under this approach, an approval for UA operations is issued contingent on the provision of an acceptable safety case. A safety case provides the "documented body of evidence" (CAA-UK, 2010) necessary to demonstrate that the risk of a MAC accident has been managed to an acceptable level (*i.e.*, meets the specified "safety-target"). To date, research has focussed on the modelling of the risk (*e.g.*, references Dalamagkidis et al. (2009), FAA (2009), Kochenderfer et al. (2010), Lum and Waggoner (2011), Melnyk (2013), NATO (2008) and Weibel and Hansman (2004)) and on the analysis of specific risk controls (*e.g.*, DAA (EUROCONTROL, 2010b; NATO, 2008; Prats et al., 2012)) at the expense of the more foundational problem of how a safety case for UA operations in non-segregated airspace should be structured and evaluated.

Haddon and Whittaker (2002) identify a number of challenges in a regulation by "safety-target" approach. Many of these challenges arise due to the lack of a method for the systematic structuring and assessment of the safety cases. In this paper, we develop the fundamental risk model describing the MAC accident scenario. The model, which builds on a comprehensive review of the state of the art in risk modelling of UA operations in non-segregated airspace, is presented in Section 2. The model is then used to systematically classify the wide array of MAC risk controls, Section 3. Over 50 common controls widely used to manage the risk of UAS operations in non-segregated airspace are classified using the model. Finally, a validation case study is presented in Section 4. The case study summarises the practical application of the framework to a real world application for an approval to operate UAS in Australian airspace. Section 5 of the paper describes some of the limitations of the model and scope for future work.

2. Modelling the MAC accident scenario

A causal model describing the sequence of states leading to a MAC has been defined in references Consiglio et al. (2012) and FAA (2009). The states are defined in terms of "separation volumes" between an UA and another aircraft. The volumes define the "performance goals" (Consiglio et al., 2012) for the respective collision avoidance and self-separation functions. The volumes are derived from existing separation standards and interpretations of regulatory concepts, and for the most part, have only been qualitatively defined. Also defined in reference FAA (2009) are "threshold volumes" that serve as triggers for the activation of particular functions (*e.g.*, collision avoidance). The chain of causal states leading to the MAC state can be described in terms of these volumes. The set of states, which are based on the volumes defined in references Consiglio et al. (2012) and FAA (2009), are illustrated in Fig. 2 and are defined as follows.

The starting state of the Air Traffic Management System (ATMS) is the state of an *Aircraft Pair*. This is the ATMS state whereby two aircraft are operational at the same time. The set of all possible *Aircraft Pairs* defines the upper limit on the number of potential encounter scenarios that may need to be evaluated. An *Aircraft Pair* is considered *relevant* when the operational volumes of the two aircraft are projected to overlap. Such a situation defines a *Traffic State*. It is important to note that in this state the aircraft are not necessarily on a collision course. As defined in reference FAA (2009), an *Intruder State* is declared when the separation between the two aircraft further reduces and the aircraft are within the ATC Separation Assurance Volume. The ATMS is in a *Threat State* when the separation between two aircraft is less than the self-separation threshold and the aircraft are on closing trajectories. The *Not Well Clear State* describes the situation when the two aircraft are within the Self-Separation Volume. The conditions defining the *Not Well Clear State* are detailed in Consiglio et al. (2012). We define here the additional state of an *Imminent Collision*, which describes the ATMS state whereby the distance between two aircraft is less than the Collision Avoidance Threshold. In accordance with FAA definitions (FAA, 2009), a